

**Relatório Final de Auditoria - RFA nº 2018005 - Ação de Auditoria nº 05 / PAINT
2018 – Gestão da Segurança da Informação e Comunicação –**

UNIDADE(S) ENVOLVIDA(S):

- **Direta(s):** Núcleo de Tecnologia da Informação – NTI
- **Indireta(s):** Todas as áreas da UFABC



1. ESCOPO DOS EXAMES

Trata-se de auditoria de natureza “mista”, ou seja, com observação aos fundamentos inerentes à auditoria de conformidade e também de natureza operacional, prevista no Plano Anual de Auditoria Interna - PAINT/2018, referente à **avaliação de diretivas e controles quanto à gestão da segurança da Tecnologia da Informação e Comunicação - TIC na UFABC**, sob os aspectos da efetividade das medidas adotadas e conformidade com as normas e diretrizes relacionadas à segurança da informação.

Cabe salientar que a realização dos exames respeitou as normas de auditoria aplicáveis à administração pública, não havendo, por parte da área avaliada, qualquer restrição aos trabalhos da Auditoria Interna - AUDIN.

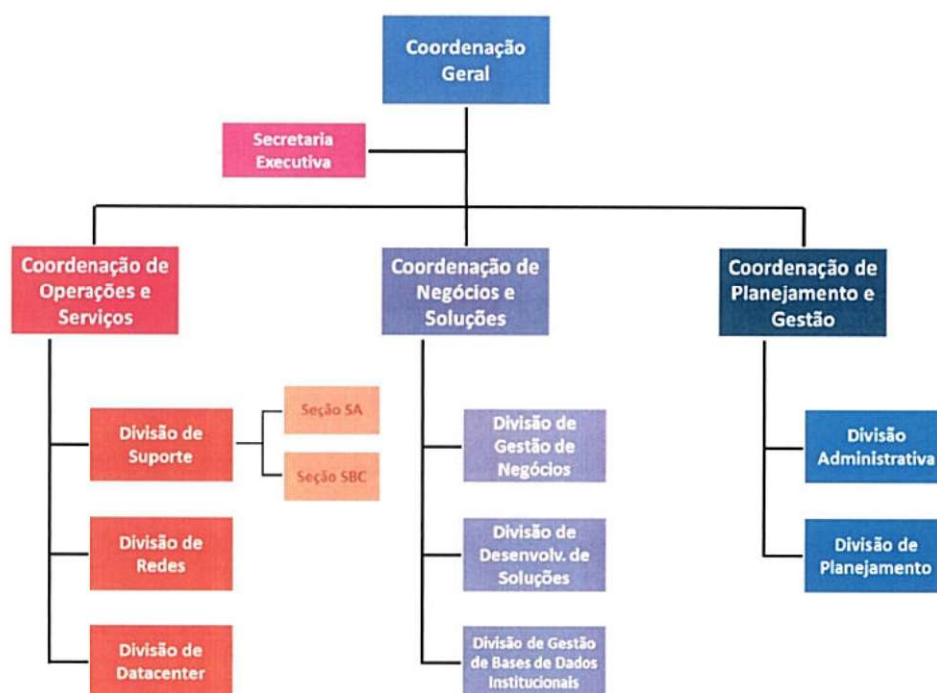
Quanto ao escopo definido, ressalta-se que a Segurança da Informação é identificada como um dos sete eixos estratégicos no Plano Diretor de Tecnologia da Informação - PDTI 2018-2020 da UFABC, além de ser elemento relevante citado no eixo intitulado ‘Governança’ do referido documento institucional, sendo que tais diretrizes também compuseram, à época, a formulação do então PDTI 2016-2017.

No tocante às operações, controle e supervisão de recursos de TIC na UFABC estão sob a responsabilidade do Núcleo de Tecnologia da Informação - NTI, e, segundo o PDTI 2016-2017 - Plano Diretor de Tecnologia da Informação anterior, a referida unidade vem paulatinamente se organizando com base em projeção estrutural proposta pelo Grupo de Trabalho - GT-NTI instituído pela Portaria nº 181, de abril de 2013, ressaltando-se ainda, no que se refere ao objeto desta auditoria, constar do referido documento a percepção de “[...] *necessidade de criação de processos e procedimentos relativos à Segurança de Informação e Comunicação de TI[...]*” (PDTI-UFABC 2016-2017, p.15).

Dessa forma, evidencia-se o papel relevante do NTI em propor normas de uso e políticas gerais de segurança da informação, além de acompanhar a execução dessas políticas pelos órgãos executivos internos (artigo terceiro, Resolução ConsUni nº 12, de 09/10/2018.)

Para maior entendimento sobre a área atualmente responsável pelo processo auditado, foi realizado um levantamento quanto à sua estrutura organizacional, como pode ser visto na Figura 1.

Figura 1 – Organograma do NTI



Fonte: Relatório de Gestão da UFABC – Exercício 2017

De forma geral, a respectiva estrutura evidencia o primeiro nível ocupado por uma Coordenação Geral assessorada por uma Secretaria Executiva, sendo a coordenação responsável pela gestão do núcleo. Além disso, o seu titular compõe também o Comitê Estratégico de Tecnologia da Informação e Comunicação – CETIC que representa instância estratégica de TIC na UFABC, além de acumular a função de Comitê de Segurança da Informação e Comunicações – CSIC, conforme previsto no artigo 9º da Política de Segurança da Informação e Comunicação - POSIC da UFABC.

O segundo nível hierárquico da estrutura possui as seguintes unidades:

- Coordenação de Operações e Serviços responsável pelo gerenciamento dos sistemas informatizados, serviços de comunicação, acesso a rede local e *internet* e integração de sistemas de *hardware* e *software*;
- Coordenação de Negócios e Soluções responsável pela gestão e entrega de soluções em automação de processos de negócios da universidade, atuando no levantamento e na definição dos processos, especificação de requisitos de negócio e de software e desenvolvimento e manutenção dos sistemas de informação;
- Coordenação de Planejamento e Gestão responsável pela gestão e planejamento das demandas de aquisições de equipamentos, serviços e suprimentos, que dão suporte aos processos de atividades-fim da UFABC.

Além das coordenações, observa-se um terceiro nível na estrutura funcional da área delineado por divisões, como se verifica na Figura 1, sendo que, especificamente quanto a Divisão de Suporte, apresenta duas seções subordinadas (quarto nível) e, geograficamente distribuídas entre os *campi*, ou seja, Seção de Suporte Santo André e Seção de Suporte São Bernardo, responsáveis por suporte técnico de equipamentos e periféricos nas salas de aula, laboratórios e salas administrativas da Universidade.

Foi realizado também um estudo sobre a distribuição de pessoal pelas áreas funcionais, obtendo-se o Quadro 1.

Observa-se que as maiores concentrações de servidores por cargo estão no cargo de Técnico de TI, aproximadamente 34%, seguidos de 23% no cargo de Analista de TI e, 20% no cargo de Técnico de Laboratório – Área de Computação e Informática, totalizando, aproximadamente 77% das lotações existentes na área.

Ao analisar mais especificamente o quadro de pessoal relacionado ao objeto dessa ação de auditoria, nota-se a existência de lotação de apenas 1 (um) único servidor no cargo de Tecnólogo na área de Segurança da Informação.

Quadro 1 – Distribuição de pessoal efetivo lotado no NTI

Quadro de Pessoal Efetivo - NTI													
Setor/Cargo	Administrador	Analista de TI	Assistente Adm.	Secretário Executivo	Técnico de Lab. - Área: Computação/Informática	Técnico de TI	Técnico em Eletrônica	Tecnólogo - Área: Eletrotécnica Industrial	Tecnólogo - Área: Rede de Computadores	Tecnólogo - Área: Segurança da Informação	Tecnólogo - Área: Sistemas Internet	Tecnólogo - Área: TI	Total / Setor
1-Núcleo de Tecnologia da Informação				1	1	1							3
1.1-Coordenação de Negócios e Soluções		1											1
1.1.1-Divisão de Gestão de Negócios		3			1	3					1		8
1.1.2-Divisão de Desenvolvimento de Soluções		4			2	1						1	8
1.1.3-Divisão de Gestão de Base de Dados Institucionais					1								1
1.2-Coordenação de Operações e Serviços		1											1
1.2.1-Divisão de Redes		3			3	4	2	1	1	1			15
1.2.2-Divisão de Data Center		3			1	2						1	7
1.3-Coordenação de Gestão e Planejamento	1		6										7
1.3.1-Divisão de Suporte		1	1		3	5							10
1.3.1.1-Seção de Suporte - Campus SA					2	8							10
Total/Cargo =	1	16	7	1	14	24	2	1	1	1	1	2	71

Fonte: Quadro elaborado pela AUDIN, com base na resposta da SUGPEPE à SA nº 34/2018.

Verifica-se ainda que, dentre outras atribuições dispostas em edital de concurso¹, destaca-se a de aplicar metodologias e ferramentas computacionais na gestão de tecnologias e de serviços de TI para incremento da segurança e confiabilidade, e de avaliação de metodologias e ferramentas para segurança da informação institucional. Sendo, portanto, uma atribuição diretamente relacionada ao escopo dessa ação.

¹ Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=01/08/2013&jornal=3&pagina=39&totalArquivos=264>;

2. METODOLOGIA

Os trabalhos transcorreram no período de 07/05 a 31/08/2018, de modo que o planejamento e a execução da ação de auditoria se amparou basicamente na legislação pertinente às tratativas de segurança da informação e comunicação - SIC, com realização de entrevistas e aplicação de questionário de conformidade referenciados pela Política de Segurança da Informação e Comunicações – POSIC da UFABC (Portaria nº 252 de 30/04/2013), na Resolução ConsUni nº 12, de 09/10/2008, Normas Complementares (NC) à IN nº 01 GSI/PR/2008 - Segurança da Informação e Comunicações e, na NBR 27002 relativa à gestão de segurança da informação, além das demais normas correlatas ao objeto de auditoria.

Foram também encaminhadas SAs às unidades internas usuárias que possuem grande tráfego de informações operacionais e/ou presença de informações sensíveis e, dentre os três centros acadêmicos, selecionou-se aleatoriamente um deles, todos com a finalidade de relacionar possíveis incidentes informacionais digitais observados pelas unidades e possíveis encaminhamentos adotados. As áreas consultadas foram: CCNH, Corregedoria, INOVA, ProAd, ProAp, ProEC, ProGrad, ProPes, PU, SG, SPO e SUGEPE.

Dessa forma, o acervo de informações resultantes dos levantamentos realizados embasaram as análises e respectivas constatações descritas no presente relatório, concentrando os trabalhos em responder às seguintes questões de auditoria:

I. A política de segurança da informação institucional está adequadamente operacionalizada?

- Política de segurança da informação - PSI;
- Política de controle de acesso – PCA; e
- Plano de continuidade de negócios – PCN.

II. A comunicação e orientação das diretrizes de segurança da informação são adequadas e efetivas?

III. A estrutura organizacional e recursos existentes são adequados para a gestão da segurança da informação digital?

Após reunidas e apresentadas as constatações verificadas pela AUDIN quanto ao escopo dos exames realizados, foi elaborado e entregue ao NTI o Relatório Preliminar de Auditoria – RPA sobre o qual a área teria um prazo de 15 dias corridos para manifestação.

Em 21/09/2018 foi realizada a reunião entre a equipe da AUDIN responsável pela ação de auditoria e a equipe do NTI responsável pelo objeto da ação no intuito de busca conjunta de soluções a respeito das constatações encontradas.

Em 08/10/2018, por meio de correio eletrônico houve manifestação parcial do NTI a respeito do RPA 2018005 e posteriormente, em 15/10/2018 foi encaminhada também por correio eletrônico uma planilha *Excel* contendo um resumo, constatação por constatação, a respeito das constatações do RPA 2018005 da presente ação.

Analisando as manifestações da área, foi elaborado o presente Relatório Final de Auditoria – RFA 2018005 no qual consta, em seu capítulo 4, as constatações apontadas, a manifestação *in verbis* do NTI, a análise da AUDIN e a recomendação para solucionar o constatado.



3. INFORMAÇÕES

A **informação organizacional é considerada um ativo relevante e crítico no contexto institucional**, sendo que o tratamento do seu manuseio, armazenamento, transporte e descarte, quando adequadamente operacionalizadas, e se balizadas por uma política de segurança da informação nas dimensões de pessoal, de processos e de tecnologia, potencializa a redução dos riscos negativos que podem ameaçar a sua integridade, confidencialidade, autenticidade e disponibilidade.

Dessa forma, a avaliação dos controles e operações existentes com relação ao objeto dessa auditoria com referência a efetividade do processo de comunicação e divulgação interna sobre as diretrizes e orientações internas decorrentes da política de segurança da informação instituída e todo o seu processo de divulgação demonstrou que **há espaço para melhorias**.

Verificaram-se fragilidades principalmente na revisão e ampliação de seus canais, de forma que haja percepção uniforme pelos colaboradores e pessoas que se utilizam das facilidades e instrumentos proporcionados pela TIC, por meio de programas adequados, como campanhas de divulgação de critérios e cuidados com a segurança da informação, com a utilização de técnicas alinhadas ao perfil do público, como *folders* eletrônicos, jogos temáticos, treinamentos, seminários, palestras, protetores de telas, páginas especializadas na *intranet*, sendo que a título de exemplo citamos o documento PSCI – Política Corporativa de Segurança da Informação do Tribunal de Contas da União - TCU apresentado em linguagem simples, direta e objetiva ou ainda, a título de exemplificação, com promoção de eventos e/ou debates em razão do evento anual do Dia Internacional de Segurança em Informática - DISI, assim como já é realizado por algumas instituições de ensino federal, como no caso do Instituto Federal de Santa Catarina - IFSC.

Outro aspecto relevante evidenciado foi a **necessidade de uma área específica de segurança da informação** ou ainda uma equipe dedicada ao assunto, uma vez que os processos que envolvem o planejamento, organização, direção e controle da segurança de informação e comunicação contemplam uma sensível e relevante função em todas as áreas da Instituição.

Destacam-se como processos relevantes que necessitam apoio institucional: o acompanhamento da efetividade da POSIC na instituição; o mapeamento dos

processos críticos organizacionais; análise de riscos e sua gestão a respeito; processo de garantia à conformidade com as diretrizes normativas e de alinhamento contínuo às melhores práticas a respeito; delineamento, acompanhamento e testes periódicos da efetividade dos planos de continuidade de negócios críticos identificados e programação; acompanhamento e difusão de uma cultura de segurança da informação e comunicação na instituição.

Além disso, considerando que a POSIC-UFABC definida pela Portaria nº 252, de 30 de abril de 2013, visa viabilizar e assegurar a segurança da informação na instituição, buscou-se por meio da análise de conteúdo da entrevista com o profissional de segurança do NTI, levantar as iniciativas existentes voltadas à formulação de processos de diagnóstico situacional quanto ao grau de maturidade organizacional em relação à segurança da informação, no que se refere à utilização dos recursos de TIC.

Assim, constatou-se que houve iniciativa positiva interna no NTI, entre os anos de 2015 e 2016, a título experimental, de formulação e aplicação de processo de levantamento, avaliação e diagnóstico da percepção da segurança da informação junto às áreas funcionais da UFABC. O referido levantamento abordou amplo espectro de temas relacionados à segurança da informação, tais como comunicação, prevenção, controle de acesso e conhecimento de normas de segurança, porém, que não trouxe resultados futuros, como possível fonte para subsídio ao processo de planejamento e de tomada de decisão a respeito do assunto. Vale mencionar que cerca de 10% do quadro de servidores respondeu à pesquisa.

Observa-se que, no decorrer da presente ação de auditoria, uma das constatações encontradas foi dirimida, uma vez que se tratava de risco quanto à repetição de divulgação de links maliciosos recebidos por *spam*. Entre o Relatório Preliminar de Auditoria – RPA e o presente Relatório Final de Auditoria – RFA, o NTI garantiu ajustar internamente seus controles de modo que o procedimento foi alterado pela equipe responsável que, a partir de então, ao realizar o alerta sobre o *e-mail (link)* malicioso, o anexará como imagem, o que impede a indução e reprodução do erro, deixando de incorrer no risco novamente em função de clique realizado inadvertidamente pelo usuário. Como essa constatação, apesar de recorrente, apresentava solução de simples implementação, que já fora acatada pela área, a AUDIN considera como solução implantada.



Cabe ainda salientar, que a Administração Pública Federal - APF e o Órgão de Controle Externo TCU mantêm amplo repositório de orientação de metodologias, procedimentos e padrões aplicados à SIC, tais como o Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações e a Cartilha de Boas Práticas em Segurança da Informação do TCU, com vistas a orientar, enquanto referências, as atividades dos gestores de SIC nas instituições federais, além do que, tais referências também integraram a base de conhecimento para a condução dos trabalhos dessa ação de auditoria.

4. CONSTATAÇÕES

Levantados pela AUDIN os achados iniciais e, encaminhados em Relatório Preliminar ao NTI, após sua manifestação e análise, restaram as seguintes constatações que merecem atenção e providências da gestão a respeito.

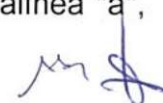
4.1.1. **Constatação 1: Fragilidades na Política de Segurança da Informação e Comunicação - POSIC da UFABC e normas internas correlatas.**

Considerando que a POSIC-UFABC visa viabilizar e assegurar a segurança da informação na instituição, buscou-se verificar a efetivação de suas diretrizes e determinações, em face de consulta de percepção e operacionalização de seus ditames por 12 unidades internas consultadas e inseridas no escopo dos exames desta ação de auditoria, uma vez que o artigo quinto da POSIC, em seu *caput*, prevê que "[...]Toda a comunidade de usuários deve observar [...]", sendo evidenciado os seguintes casos específicos:

1º) **Não há uniformização entre as unidades de tratamento seguro de acesso às informações.** Em que pese todas as unidades relatarem que seus colaboradores acessam os recursos computacionais por meio de 'senha', apenas 2 unidades orientam seus colaboradores à criação de senhas 'fortes', 1 unidade orienta seus colaboradores a não divulgação de informações em razão do cargo, 1 unidade possui 'termo de sigilo' junto àqueles que tem contato com informações sigilosas e 1 unidade orienta suas chefias para realizarem a troca periódica de senhas de e-mails;

2º) **Falta de clareza de procedimentos, supervisão e interação quanto ao encaminhamento de ocorrências de incidentes de segurança da informação.** Por meio dos relatos de sete unidades, evidenciou-se que não há previsão formal de interação processual estabelecida com atores internos (CSIC, ETIR) previstos na POSIC para o registro de incidentes de segurança da informação.

Além disso, foi evidenciado por meio de resposta à SA nº 46/2018 a inexistência de instalação de uma comissão de auditorias de TIC para supervisionar os sistemas da UFABC, conforme previsão disposta no art. 5º, inciso V, alínea "a", da POSIC - UFABC.



Cabe ressaltar, que quanto às atribuições institucionais do NTI, a referida unidade além de ter a competência institucional de gerir as plataformas e serviços de TIC na instituição, também tem a função prevista pela referida POSIC, em seu art. 8º, de atuar "[...] como Gestor de Segurança da Informação e Comunicações (GSIC)[...]" e que dentre as competências previstas ao GSIC, segundo a Norma Complementar (NC) nº 03/IN01/DSIC/GSIPR, item 5.3.7.2, alínea "g", cabe "[...]Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF[...]"; além disso, a Resolução ConsUni nº 12, de 09/10/2008, prevê em seu artigo 2º que "[...]A abrangência da segurança é definida pelo Núcleo de Tecnologia da Informação (NTI), no tocante as responsabilidades das Unidades, Centros, Laboratórios ou outros setores integrantes da UFABC[...]";

3º) Ausência de estruturação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)

A POSIC-UFABC prevê em seu art. 10º a instituição de equipe de tratamento e resposta a incidentes em redes computacionais e que essa deve ser instituída, conforme previsto em seu art. 8º, formalmente pelo Gestor de Segurança da Informação e Comunicações (GSIC). Tal previsão é corroborada por similar determinação prevista no item 5.3.7.4 da Norma Complementar nº 03/IN01/DSIC/GSIPR. Cabe observar que a publicação da POSIC UFABC foi no ano de 2013 e que o PDTI 2014-2015 já previra, a partir de análise SWOT realizada à época, como um dos pontos fracos levantados, a "[...]Inexistência de área e equipe dedicada à Segurança da Informação[...]"; (PDTI 2014-2015, p. 21), ainda em que pese outros pontos levantados à época revelarem maior criticidade a partir de uma análise por meio da aplicação da ferramenta de qualidade de Matriz de Priorização GUT - Gravidade, Urgência e Tendência.

Dessa forma, a fim de diagnosticar a situação atual a respeito dos componentes e procedimentos existentes em torno do assunto foi conduzida entrevista com profissional de segurança da informação do NTI, sendo que a partir da análise de seu conteúdo, constatou-se a ausência de estruturação formal da ETIR na instituição.



Assim, cabe acrescentar que a Corte de Contas da União já pacificou a necessidade de instituição formal de tal componente organizacional, ou seja, o ETIR, como pode ser conferido nos julgados: Acórdão TCU 381/2011-Plenário, item 9.1.1; Acórdão TCU 594/2011-Plenário, item 9.4.7; e Acórdão TCU 866/2011-Plenário, item 9.2.6.

4º) **Ausência de Plano de Continuidade de Negócios - PCN formalizado.**

Em face de a POSIC prever em sua alínea 'a', do inciso IV, do caput do artigo 5º que

"**Toda a Comunidade de usuários** deve observar que:

[...]

IV. quanto à gestão de continuidade:

a) **prever um plano de continuidade de negócios para manter a disponibilidade dos serviços de tecnologia de informação e comunicações**, incluindo o uso de redundância em sua implantação".(Grifos adicionados)

E, considerando que por plano de continuidade de negócios, o item 4.10 da Norma Complementar 06/IN01/DSIC/GSI/PR a define como sendo a

[...] **documentação dos procedimentos e informações necessárias** para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo **num nível previamente definido, em casos de incidentes** (grifos acrescentados)

Foi conduzida entrevista com profissional de segurança da informação do NTI e, por meio da análise de seu conteúdo, ficou evidenciado que, apesar da existência de ambientes redundantes e sistema de *backup*, a inexistência formal de plano de continuidade de negócios na instituição. E ainda que inexistente programa de treinamento interno de caráter preventivo para tratamento, condução e recuperação de incidentes.

A respeito da importância desse tema e a título de exemplificação, o TCU emanou os seguintes acórdãos: Acórdão TCU 782/2004 - 1ª Câmara, itens 9.2.4 e 9.3.4; Acórdão TCU 1382/2009 – Plenário, item 9.2; e Acórdão TCU 1137/2012 - 2ª Câmara, item 1.4.1.2.

5º) **Fragilidade no processo de controle de acessos.**

Foi testada a efetivação do controle de acesso interno, sendo constatadas as seguintes fragilidades: a existência de 'senhas genéricas', onde mais de um profissional utiliza a mesma senha para acesso a determinados recursos de TIC e,

em resposta à SA nº 30/2018, na qual solicita em seu item 3.1 o fornecimento de relação de usuários que possuem *status* de administradores de sistemas, foram evidenciadas as seguintes ocorrências:

a) Siape nº [REDACTED] – verificou-se que houve vacância de cargo por posse em outro cargo inacumulável (BS nº 715 de 16/01/2018) e consta atualmente como administradora do SIE;

b) Siape nº [REDACTED] – verificou-se afastamento para participação em programa de pós-graduação *stricto sensu* de 28/05/2018 a 27/05/2020 e consta com acesso a usuário *root* / servidor DHCP

c) Siape nº [REDACTED] – verificou-se que houve vacância de cargo por falecimento (BS nº 604 de 11/11/2016) e consta atualmente como administrador do sistema de "Inscrições em Cursos";

d) Siape nº [REDACTED] – verificou-se que houve exoneração, a pedido, (DOU de 03/06/2016) e consta como administrador do servidor de impressão;

e) Foi evidenciado, com base em análise documental, atribuição à pessoa exercendo estágio curricular com perfil de acesso como usuário *root* ao servidor de impressão durante o primeiro semestre do ano de 2014.

4.1.2. Manifestação da área: Manifestação enviada por meio de duas mensagens de correios eletrônicos encaminhadas em 08/10 e 15/10/2018 pelo NTI à AUDIN em resposta ao RPA 2018005:

O relatório retrata fielmente o quadro da área da segurança da informação, se é que pode se referir desta forma, já que não existe uma divisão de segurança da informação na UFABC.

Como eu respondi na entrevista, o fato de não haver uma estrutura mínima da área de segurança da informação desencadeou todos os outros problemas relatados, como por exemplo, a ausência de uma "ETIR" e, conseqüentemente, a ausência de procedimentos para notificação e tratamento de incidentes de segurança da informação. Os direitos de acesso de cada usuário serão revistos periodicamente. Esta regra está prevista na norma de controle de acesso que aguarda a aprovação no CETIC.

A nova Política de Segurança da Informação e a norma de controle de acesso que aguardam aprovação no CETIC tratam estas questões, incluindo a prática de conscientização. A nova política de segurança da informação que aguarda a aprovação no CETIC irá tratar questões sobre a criação de uma equipe de tratamento incidentes (ETIR) e CSIC que deverá formalizar o procedimento.

O Plano de Continuidade de Negócios (PCN) também está previsto na nova Política de Segurança da Informação que aguarda a aprovação no CETIC.

4.1.3. Análise da AUDIN: Em que pese a manifestação do gestor, a Auditoria Interna mantém a constatação. As considerações apresentadas corroboram o entendimento constante do Relatório Preliminar de Auditoria. Será realizado monitoramento para verificação quanto à aprovação da nova Política de Segurança da Informação e Comunicação – POSIC que, segundo o gestor, está em pauta no CETIC e, irá dirimir todas as fragilidades apontadas.

4.1.4. Recomendações: Certificar-se de que as novas Políticas e Normas mencionadas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC. A área deverá definir data (dia/mês/ano) para realização de monitoramento, por parte da AUDIN, quanto às providências informadas.

4.1.5. Constatação 2: Fragilidade na aderência às orientações da NBR ISO/IEC 27002 - Gestão da Segurança da Informação.

Considerando que a POSIC define que a gestão SIC da UFABC deve observar inclusive a NC nº 03/IN01/DSIC/GSIPR e que, por sua vez, se baseia, dentre outras, na NBR ISO/IEC 27002 a qual trata do código de prática para gestão de SIC, sendo inclusive uma das normas recorrentemente citadas pelo TCU, uma vez que a referida Corte de Contas entende que "[...] configura-se como um dos melhores critérios de auditoria de segurança da informação[...]" (Cartilha de Boas Práticas em Segurança da Informação, 4ª Ed. p.39), buscou-se, assim, verificar a conformidade das práticas existentes de gestão interna da segurança da informação.

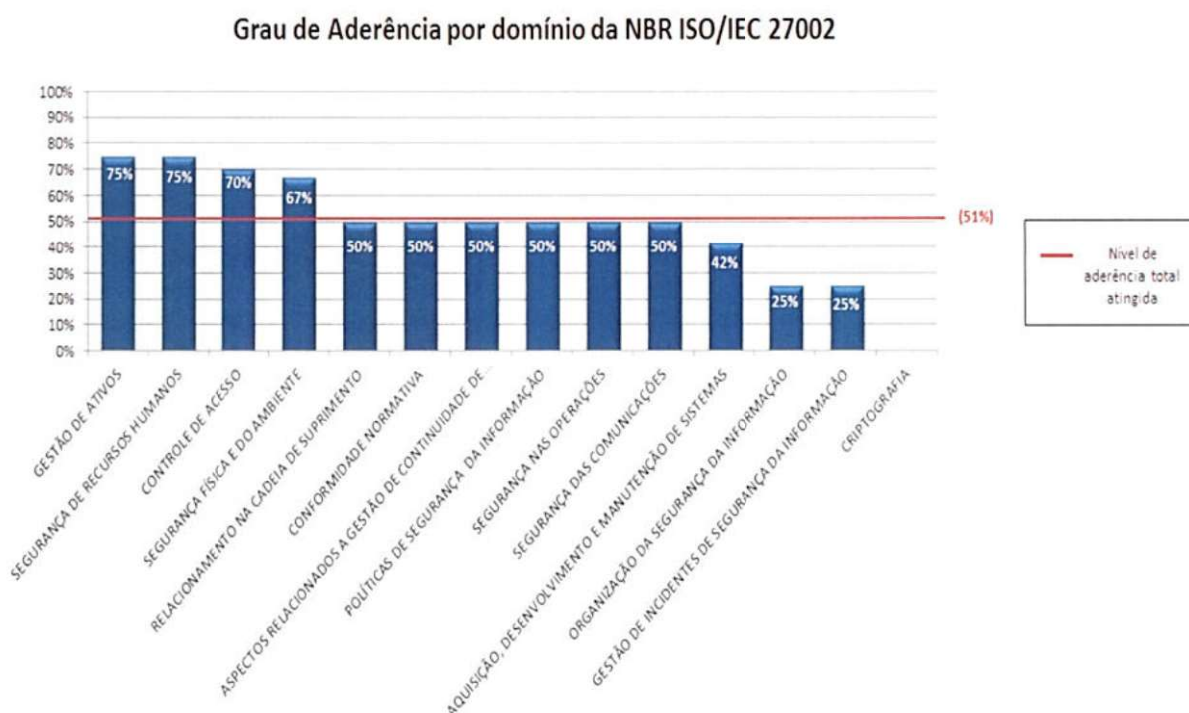
Para tanto, foi realizada entrevista baseada na legislação pertinente e nas boas práticas de segurança da informação com o profissional de segurança da informação do NTI. E, também a ele, aplicado um teste de conformidade² referenciado pelos preceitos da norma regulamentadora - NBR ISO/IEC 27002, composto por 58 quesitos e que abrangem 14 domínios, a saber: Políticas de segurança da informação, Organização e segurança da informação, Segurança de RH, Gestão de ativos de TIC; Controle de acesso, Criptografia, Segurança física e do ambiente, Segurança nas operações, Segurança das comunicações, Aquisição, manutenção e desenvolvimento de sistemas, Relacionamento na cadeia de

² Teste de conformidade adaptado ao ambiente da UFABC a partir do *framework* sugerido na obra 'Gestão da Segurança da Informação - Uma visão executiva' (Marcos Sêmola, Ed. Campus, 2ª edição).

suprimentos, Gestão de incidentes de segurança da informação, Aspectos relacionados à gestão de continuidade de negócios e Conformidade às normas.

Cada um dos quesitos³ foi respondido pela área mediante a sua existência total, parcial ou ainda a inexistência de efetividade do quesito na UFABC, onde: aos primeiros foram atribuídos 2 pontos, para os segundos 1 ponto e para os últimos 'zero' ponto, no caso de sua inexistência.

A partir de então, foi possível extrair por domínio de assunto que compõe a referida norma regulamentadora, os seguintes percentuais de aderência, conforme demonstrado no gráfico abaixo:



Fonte: Elaborado pela AUDIN⁴.

Conforme apresentado, a pontuação total de aderência atingida em face das respostas oferecidas pela área aos quesitos propostos foi de aproximadamente 51%, ou seja, 49% das práticas recomendadas pela NBR ISO/IEC 27002 não são implementadas internamente, merecendo tal resultado atenção da gestão quanto ao alinhamento pleno às conformidades normativas, principalmente no que tange aos domínios que estão abaixo do grau de aderência total apurado de 51%, ou seja, os

³ Dos 58 quesitos propostos, apenas 1 não foi respondido pela área;

⁴ Baseado em diretrizes conceituais do livro Gestão da Segurança da Informação – Uma visão executiva, Marcos Sêmola, 2014, 2ª Edição, Elsevier Editora Ltda.

domínios de Relacionamento da cadeia de suprimentos, de Conformidade normativa, de Aspectos relacionados à gestão de continuidade de negócios, de Política de segurança da informação, de Segurança nas operações, de Segurança nas comunicações, de Aquisição, desenvolvimento e manutenção de sistemas, de Organização da Segurança da informação, de Gestão de incidentes da segurança da informação e de Criptografia de informações sensíveis, uma vez que apresentaram índices abaixo da pontuação total atingida.

4.1.6. Manifestação da área: Manifestação enviada por meio de duas mensagens de correios eletrônicos encaminhadas em 08/10 e 15/10/2018 pelo NTI à AUDIN em resposta ao RPA 2018005:

A conformidade das práticas existentes de gestão de segurança da informação com base na norma ISO NBR 27002 será realizada periodicamente após da estruturação da área de segurança da informação com a nomeação do seu gestor que se dará com a aprovação da nova Política de Segurança da Informação que está sendo discutida no CETIC.

A minha ressalva se faz necessária exatamente no aspecto do relatório pelo qual foi mensurado o grau de aderência aos domínios da norma NBR ISO/IEC. É no mínimo estranho eu me deparar com 25% de aderência do domínio da gestão de segurança, pois as praticas recomendadas neste domínio é praticamente nula, visto que não há um Gestor de Segurança da

Informação, bem como não há um Comitê de Segurança da Informação, embora o CETIC tenha incorporado esta função de forma falha. Além disso, o índice de aderência aos domínios de Gestão de Ativos, Segurança de Recursos Humanos, Controle de Acesso, Segurança Física e do meio ambiente e conformidade normativa não condiz com a realidade. Não chega a 50%. É possível que o levantamento realizado não tenha considerado todos os detalhes técnicos para a mensuração, pois um levantamento realizado nos mesmos moldes em outubro de 2015 retornou um resultado bem inferior. O resultado pode ser visualizado na imagem em anexo retirada da análise crítica da segurança da informação realizada no mesmo ano. Apesar de o resultado expressar a realidade de 2015, muito pouco se evoluiu para já alcançar níveis considerados satisfatórios como demonstra o relatório. A metodologia escolhida para levantar o nível de aderência à ISO NBR 27002 em 2015 levou em consideração 4 níveis de conformidade, sendo: Não implementado; Planejado; Atende Minimamente; e Atende completamente. Uma verificação anterior realizada no início de 2015 considerou cinco níveis de mensuração, existindo também o nível em que a pratica, além de atender completamente, é referencia no mercado. Este nível foi retirado por ser considerado excessivo.

4.1.7. Análise da AUDIN: Ressalta-se que o grau de aderência apresentado foi medido de acordo com o parâmetro da literatura mencionada, o que não impede que resultados diferentes venham a ser obtidos com a utilização de outras técnicas e ou literaturas, como foi o caso mencionado pelo próprio respondente do questionário, que alerta haver uma aderência ainda menor que a obtida com a técnica utilizada pela AUDIN, corroborando com a urgente necessidade de a UFABC dedicar-se ao tema.

4.1.8. Recomendações: Certificar-se de que as novas Políticas e Normas mencionadas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC. A área deverá definir data (dia/mês/ano) para realização de monitoramento, por parte da AUDIN, quanto às providências informadas.

4.1.9. Constatação 3: Falhas na Comunicação e Divulgação da SIC pelo NTI.

Em que pese ter-se verificado no site do NTI, mais especificamente no espaço destinado à Segurança de Informação e Comunicação, um documento intitulado "Cartilha de Segurança para Internet", que trata especificamente de dicas de segurança para escolha e proteção de senhas, ressalta-se que são necessárias divulgações de maior amplitude sobre o tema e que sejam realizadas de forma completa e periodicamente para que se tornem efetivas. Tal diretriz se suporta na Instrução Normativa - IN/GSI/PR nº 01/2008, a qual estabelece em seu Inciso I, do Artigo 7º, a necessidade de promover uma "(...) cultura de segurança da informação e comunicações (...)" e, para tanto, a ausência de um Manual / Cartilha completa sobre SIC bem como a ausência de sua ampla e periódica divulgação contribuem para o descumprimento do normativo.

Destarte, foram solicitadas por meio da Solicitação de Auditoria - SA nº 31/2018 informações a respeito de como é realizada a divulgação da Segurança da Informação e Comunicação - SIC na Universidade pelo NTI, sendo a área atualmente responsável pela matéria na UFABC. Em resposta, encaminhada por mensagem eletrônica à AUDIN, em 19 de julho de 2018, o NTI informa que realiza as ações de divulgação por meio basicamente da página eletrônica do NTI na Internet, em espaço próprio da SIC (<http://nti.ufabc.edu.br/seguranca-da-informacao>). Porém, em acesso ao *link* disponibilizado, verificaram-se algumas falhas enumeradas a seguir:

a) Na respectiva página é citado o e-mail "abuse@ufabc.edu.br" para que se denuncie pirataria ou quaisquer incidentes de segurança e, em entrevista realizada em 01/08/2018 com o único Analista de Segurança da Informação na UFABC, foi informado que o referido e-mail trata-se de norma e protocolo internacional sobre SIC e que em qualquer lugar do mundo os especialistas na área saberão que devem utilizar este canal. Porém, cabe ressaltar que, ao situar-se em uma Universidade e

ter como clientes toda uma Comunidade Acadêmica, a SIC deve alcançar a todos, assim como sua divulgação, sendo que a existência desse canal, apesar de estar explícita na página eletrônica e, ser divulgada no rodapé do corpo do e-mail pelo qual o NTI faz algum alerta de SIC, quando necessário, não basta. Na própria AUDIN, servidores comuns, administradores, advogados, economistas, não sabiam da existência desse canal e também não souberam como proceder em relação à informação sobre "chave PGP" que se encontra logo a seguir da indicação do canal na referida página eletrônica de SIC/NTI. Isso demonstra que a comunicação/divulgação não está sendo efetiva, pois não atinge ao seu público alvo;

b) A área de SIC na página do NTI (acessada em 07/08/2018 às 09h00) possui 7 (sete) *links*, sem maiores explicações sobre eles:

1) O primeiro deles trata-se da versão "pdf" da POSIC, porém, essas informações são obtidas somente se o usuário/cidadão/cliente clicar no *link*, pois ele encontra-se apenas identificado por sua sigla "POSIC UFABC 2013", sem qualquer menção sobre o que se trata e qualquer destaque sobre sua importância;

2) O segundo *link* é um trecho de uma Cartilha de Segurança para *Internet* que se refere ao cuidado que o usuário deve ter com suas senhas. Está identificado como "Cartilha de Segurança para Internet - Fascículo senhas", sendo um documento em formato '*power point*' que contém informações relevantes sobre como elaborar uma senha segura, principais riscos, etc., porém, encontra-se publicado na página, mas sem maiores divulgações a respeito;

3) O terceiro *link* abriga as "Normas de uso do correio eletrônico" como documento em formato 'pdf' contendo a publicação, cuja existência perfaz quase 2 (dois) anos, mas não alcançou a divulgação necessária para atingir seu objetivo, não sendo essa devidamente aplicada por todos da Comunidade;

4) O quarto *link* trata de "Recomendações mínimas de segurança para computadores de trabalho da UFABC", sendo um documento que contém informações relevantes sobre atualização e manuseio pelo usuário do sistema antivírus instalado em sua máquina. Também, apesar de publicado na página, não tem sido divulgado por outros meios ou de forma contínua e efetiva;

5) O quinto *link* da referida página é identificado como "Resolução nº 12 do CONSUNI", a qual o Conselho Universitário aprova as Normas de Uso e Políticas Gerais de Segurança da UFABC, porém apresenta somente a sigla, sem maior

descrição e o referido link não leva ao documento citado, mas sim à página de "Últimas Notícias" do NTI, prejudicando a transparência e o acesso;

6) O sexto *link* intitulado "Ações de Segurança na Rede" leva a um aviso do NTI para o bloqueio de acesso dos usuários da Comunidade Acadêmica a determinados *sites* (*streaming* de vídeos) pelos microcomputadores corporativos a partir de então, o qual não foi amplamente divulgado perante todos os usuários;

7) O sétimo e último *link* aparece como "PGP Public Key" sobre o qual consta apenas a seguinte informação: "*Denuncie a pirataria e reporte incidentes de segurança: abuse@ufabc.edu.br. Para comunicação através de um canal seguro, por favor, utilize a seguinte chave PGP: PGP Key ID: 53BFF5D4 Fingerprint: CB17 7524 3041 D5C6 04A7 D562 585F 69CC 53BF F5D4*", cujo *link* leva a uma outra página, repleta de códigos, o que atrapalha a comunicação e entendimento, tornando-a inefetiva perante a maioria do público na Universidade.

Dessa forma, o principal canal citado pelo NTI como meio pelo qual realiza a divulgação de SIC na UFABC, apesar de explícito, publicado em sítio eletrônico de Internet tem se demonstrado ineficiente perante seu público alvo.

4.1.10. Manifestação da área: Manifestação enviada por meio de duas mensagens de correios eletrônicos encaminhadas em 08/10 e 15/10/2018 pelo NTI à AUDIN em resposta ao RPA 2018005:

A falha na comunicação e divulgação da SIC pelo NTI (...) será resolvida indiretamente quando a estrutura organizacional de segurança da informação for aprovada pelo CETIC, pois a área de segurança da informação precisa existir para que haja ações e para as mesmas sejam divulgadas. As poucas ações divulgadas até hoje partiram de iniciativa própria e isolada, portanto, sem procedimentos, e motivadas pela importância do tema. Qualquer funcionário do NTI poderia ter feito esta publicação; Vale ressaltar que o problema de comunicação também atinge todas as áreas da UFABC e não apenas o NTI, pois as pessoas não leem o que foi publicado no nosso site por questões culturais. Por exemplo, a UFABC não possui uma intranet e o Boletim de Serviço é um modelo de comunicação bem falho e não atinge cerca de 10% dos funcionários.

O NTI tem estudado ações de gestão da comunicação institucional para o seu portal com a finalidade de dar maior visibilidade às suas publicações. O NTI estuda melhorar a sua comunicação por meio de ações como palestras, boletins, entre outros. Este estudo ocorre em paralelo à criação de um escritório de Governança de TIC que será responsável por esta gestão e que atualmente está na fase beta.

4.1.11. Análise da AUDIN: Em que pese a manifestação do gestor, a Auditoria Interna mantém a constatação. As considerações apresentadas corroboram o entendimento constante do Relatório Preliminar de Auditoria. Será realizado

monitoramento para verificação quanto à criação do “escritório de governança” e o cronograma que contemple o conjunto de ações citadas para a melhoria necessária à comunicação e divulgação institucional em relação ao tema SIC na UFABC que, segundo o gestor, está em fase de estudos e testes e, assim que implantadas, irão dirimir todas as fragilidades apontadas.

4.1.12. Recomendações: Certificar-se de realizar um plano de trabalho, com seu devido cronograma para implantação do conjunto das ações mencionadas e que elas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC. Além de definir data (dia/mês/ano) para realização de monitoramento por parte da AUDIN quanto às providências propostas pelo NTI.

4.1.13. Constatação 4: Ausência de estrutura e recursos de SIC na UFABC.

Em todos os itens verificados quando à Segurança da Informação e Comunicação - SIC na UFABC, constatou-se a ausência de estrutura específica e recursos adequados destinados ao tema.

No que tange à estrutura, em reuniões realizadas com a Coordenação do NTI e, em respostas às Solicitações de Auditoria – SAs nº. 34 e 35/2018, foi informado que a UFABC conta apenas com um único servidor da área de SIC, um Técnico na área de Segurança da Informação e que, ainda segundo o NTI, não há estrutura física específica para tratar o assunto na Universidade, nem mesmo outros servidores dedicados a esta função. O referido servidor está lotado na Divisão de Redes compartilhando seu tempo com outros temas à parte da SIC.

Assim, com relação à estruturação de área ou equipe própria para tratamento de assuntos de SIC, o Manual de Boas Práticas em Segurança da Informação do TCU recomenda:

"[...]É recomendável que na estrutura da instituição exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar funções de segurança[...]"

A Secretaria de Fiscalização de Tecnologia da Informação – Sefti, em 2007, realizou auditoria junto a órgãos e entidades da Administração Pública Federal - APF que teve como resultado o Acórdão 1.603/2008 - Plenário TCU, que, dentre outras, traz a recomendação de nº 9.1.3 ao Conselho Nacional de Justiça - CNJ e ao

Conselho Nacional do Ministério Público - CNMP:

"(...)9.1.3. orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a **área específica para gerenciamento da segurança da informação**, a política de segurança da informação e os procedimentos de controle de acesso(...)" (Grifos adicionados).

E quanto ao recurso orçamentário, a situação atual encontra-se em desconformidade perante a legislação vigente, segundo a qual a Administração deve "[...] **III - propor programa orçamentário específico para as ações de segurança da informação e comunicações [...]**" (Artigo 5º, inciso III, Instrução Normativa - IN/GSI/PR nº 1, de 13 de junho de 2008 - grifos adicionados).

Cabe ainda mencionar que a referida IN, em seu artigo quinto, prevê um arcabouço de gerenciamento específico de SIC, ainda inexistentes na UFABC.

4.1.14. Manifestação da área: Manifestação enviada por meio de duas mensagens de correios eletrônicos encaminhadas em 08/10 e 15/10/2018 pelo NTI à AUDIN em resposta ao RPA 2018005:

O relatório retrata fielmente o quadro da área da segurança da informação, se é que pode se referir desta forma, já que não existe uma divisão de segurança da informação na UFABC.

Como eu respondi na entrevista, o fato de não haver uma estrutura mínima da área de segurança da informação desencadeou todos os outros problemas relatados.

A estruturação da área de segurança da informação com a nomeação do seu gestor se dará com a aprovação da nova Política de Segurança da Informação que está sendo discutida no CETIC.

4.1.15. Análise da AUDIN: Em que pese a manifestação do gestor, a Auditoria Interna mantém a constatação. As considerações apresentadas corroboram o entendimento constante do Relatório Preliminar de Auditoria.

4.1.16. Recomendações: Certificar-se de que as novas Políticas e Normas mencionadas atendam a todos os pontos de controles necessários, sendo publicadas, amplamente divulgadas, de fato exercidas, periodicamente monitoradas e realmente efetivas quanto a garantir a integridade da SIC na UFABC e, certificar-se ainda que, a criação da devida estrutura organizacional proposta seja devidamente efetivada. A área deverá definir data (dia/mês/ano) para realização de monitoramento, por parte da AUDIN, quanto às providências informadas.



5. CONCLUSÃO

As atividades da Auditoria Interna da UFABC são planejadas para produzir informações tempestivas e apropriadas que auxiliem os gestores nos processos de tomada de decisão e no gerenciamento de riscos, na forma prevista no referencial técnico de atividade de auditoria interna governamental.

A adoção de controles internos adequados é de fundamental importância ao aprimoramento dos processos relacionados à Segurança da Informação e Comunicação na medida em que **permite segurança a todas as informações estratégicas da instituição**, a adoção de boas práticas, observância às normas aplicáveis e proteção aos sistemas, acesso a redes e pastas compartilhadas e a consequente garantia de uma integridade dessas informações na tomada de decisões.

Assim sendo, os apontamentos deste relatório de auditoria indicam serem **necessários esforços da área responsável, bem como da Alta Administração**, para **aprovação de uma Política de Segurança da Informação e Comunicação e regras internas complementares** que atendam às necessidades crescentes da Universidade. As prescrições de providências aqui apontadas, necessárias a esses ajustes, visam assegurar a confidencialidade, disponibilidade e integridade das informações eletrônicas no âmbito institucional, tendo em vista que o constante crescimento de dispositivos e demandas que se utilizam dos serviços provenientes dos ativos de informação e comunicação atrela, por conseguinte, riscos que podem impactar negativamente o regular processamento de suas operações e serviços, em razão das constantes e novas ameaças do dinâmico ambiente da tecnologia da informação e comunicação.

Espera-se, portanto, com o presente trabalho de Auditoria Interna, a busca de soluções para os apontamentos realizados, com o devido patrocínio da alta gestão, de modo que a relevante função de Segurança de TIC na UFABC passe a contemplar o sua verdadeira relevância no âmbito corporativo, de modo a subsidiar os objetivos institucionais desejados.



6. ENCAMINHAMENTOS:

Encaminha-se três vias deste Relatório Final de Auditoria - RFA:

a) Ao Núcleo de Tecnologia da Informação para conhecimento e manifestação final do gestor **no prazo de 15 dias**, acerca das conclusões da Auditoria Interna, bem como o **preenchimento do documento intitulado "Plano de Providências" – PP**, conforme modelo Anexo I deste relatório, indicando as ações e os prazos previstos para sua implementação no atendimento às recomendações nele constantes;

b) Ao Magnífico Reitor, para ciência e atuação que julgar necessária, em face do teor deste Relatório; e

c) À Controladoria-Geral da União - CGU, em atendimento ao disposto no artigo 15, da IN/CGU nº 9, de 9 de outubro de 2018 e, atendimento ao item 27, do Capítulo II, do Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, aprovado pela IN/CGU nº 3/2017.

Santo André, 31 de outubro de 2018.



Patricia Alves Moreira
Administradora

De acordo. Encaminhe-se, conforme o proposto.



Rosana de Carvalho Dias
Gerente da Auditoria Interna da UFABC.

EM BRANCO

Modelo de Plano de Providências - PP



Unidade responsável: Núcleo de Tecnologia da Informação - NTI

Relatório de Auditoria nº 2018005 – Ação de Auditoria na Segurança de TIC.

1.a. Constatação 1: Fragilidades na Política de Segurança da Informação e Comunicação - POSIC da UFABC e normas internas correlatas.

1.b Providências a serem Implementadas: _____.

1.c. Prazo de Atendimento: ____/____/____.

2.a. Constatação 2: Fragilidade na aderência às orientações da NBR ISO/IEC 27002 - Gestão da Segurança da Informação.

2.b Providências a serem Implementadas: _____.

2.c. Prazo de Atendimento: ____/____/____.

3.a. Constatação 3: Falhas na Comunicação e Divulgação da SIC pelo NTI.

3.b Providências a serem Implementadas: _____.

3.c. Prazo de Atendimento: ____/____/____.

4.a. Constatação 4: Ausência de estrutura e recursos de SIC na UFABC.

4.b Providências a serem Implementadas: _____.

4.c. Prazo de Atendimento: ____/____/____.

Santo André, ____ de _____ de 2018.

_____ (assinatura do responsável)

Nome do Responsável:

Cargo/Função:

EM BRANCO